Background

Who is local administrator is configured in each domain-joined computer. It is therefore not possible to ask the DC for that information, instead it needs to be queries from each computer. The local group `Administrators` can contain domain groups. This can create unforseen complexity that accidentally adds users to the local Administrators group.

A user who is local administrator on a hosts leverage this privilege in a number of different ways. It can, for example, be used to extract credentials from the lsass process (See Credential Extraction for how to perform that attack).

Pre-requisites

Valid domain user.

Risks

Only run in bloodhound, so no risks.

How to check for

Using Bloodhound

For installing and running Bloodhound see Tools

Bloodhound enumerates this information. To check where your user is local admin you can just search for your user and then click on it and check the information. For example:

```
 Local Admin Rights
First Degree Local Admin 0
Group Delegated Local Admin Rights 3
Derivative Local Admin Rights 5
```

Find what groups have local admin rights

```
MATCH p=(m:Group)-[r:AdminTo]->(n:Computer) RETURN m.name, n.name ORDER BY m.name
```

Find what group has most local admin rights and list them in that order:

```
MATCH p=(m:Group)-[r:AdminTo]->(n:Computer) RETURN m.name, count(m.name) ORDER BY count(m.name) desc
```

Find what users have local admin rights, and on which computers:

```
MATCH p=(m:User)-[r:AdminTo]->(n:Computer) RETURN m.name, n.name ORDER BY m.name
```

Find how many users in total have local admin access to resource:

```
MATCH p=(m:User)-[r:AdminTo]->(n:Computer) RETURN count(distinct m.name)
```

Find the users that is local admin on most machines:

```
MATCH p=(m:User)-[r:AdminTo]->(n:Computer) RETURN m.name, count(m.name) ORDER BY count(m.name) desc
```

Check to see that there are no unresonable amount of groups and users that are local admins. Also check that the domain controllers

Using PowerView

For installing and running PowerView see Tools

```
Find-LocalAdminAccess
```

Using Crackmapexec

How to exploit

Recommendation

Related Vulnerabilities

References